(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 October 2003 (09.10.2003)

PCT

(10) International Publication Number
WO 03/084175 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/SG02/00049

(22) International Filing Date: 27 March 2002 (27.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant and
(72) Inventor *(for all designated States except US)*: **BARRACUDA INNOVATIONS PTE LTD.** [SG/SG]; 151 Chin Swee Road #03-03/04, Manhattan House, Singapore 169876 (SG).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **CHEW, Chin, Nyuk** [SG/SG]; Blk 307, Woodlands Avenue 1 #11-301, Singapore 730307 (SG).

(74) Agent: **LEE, Chiat, Jin, Jeffrey**; Kweh Lee & Partners, 151 Chin Swee Road #03-03/04, Manhattan House, Singapore 169876 (SG).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

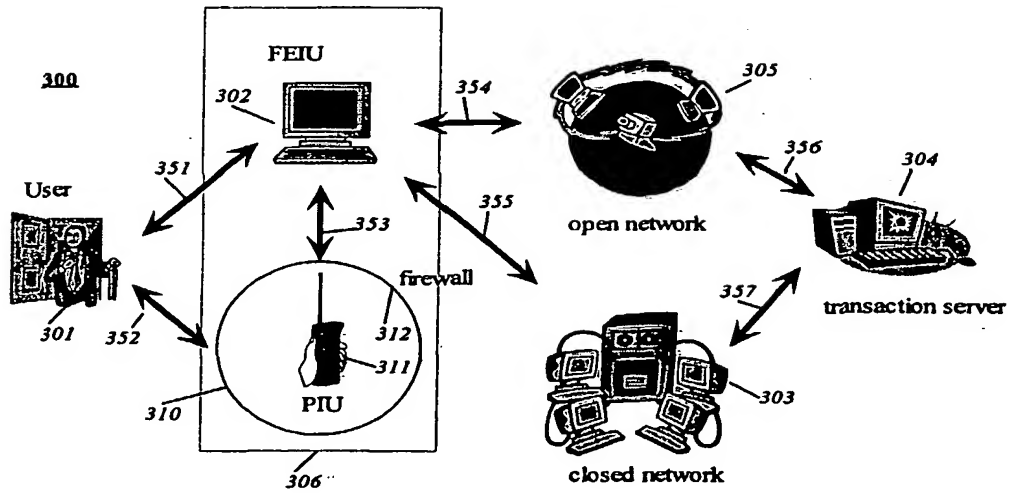
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG,*

[Continued on next page]

(54) Title: A SYSTEM AND METHOD FOR SECURE ELECTRONIC TRANSACTION USING A REGISTERED INTELLIGENT TELECOMMUNICATION DEVICE



301 UTILISATEUR
312 PARE-FEU
303 RESEAU FERME
304 SERVEUR DE TRANSACTION
305 RESEAU OUVERT

(57) Abstract: A system, method and apparatus that enables the provision of identification, authentication, encryption and non-repudiation in an electronic transaction environment between a transaction client and a transaction server. The transaction client comprises a registered telecommunication-based Portable Intelligent Unit (PIU) as a distributed component having a direct communication and transaction with a separate local microprocessor-based Front End Intelligent Unit (FEIU). The Front-End-IU has access to an open or closed network, but may contact the transaction server directly.

WO 03/084175 A1

UZ, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)
of inventorship (Rule 4.17(iv)) for US only

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A SYSTEM AND METHOD FOR SECURE ELECTRONIC TRANSACTION USING A REGISTERED INTELLIGENT TELECOMMUNICATION DEVICE

BACKGROUND OF THE INVENTION

Technical Field

01 The present invention concerns a system and method for a secure electronic transaction system or derivatives of this method. More particularly, the system and method involves the use of a registered intelligent telecommunication device as a distributed component with direct communication and transaction with a separate local microprocessor-based device that has access to an open or closed network. An objective of the system and method is to provide one or more of four basic requirements, including identification, authentication, encryption and non-repudiation.

Description of the Related Art

02 Identification and authentication are core components for most types of access control, whether for communications, business transactions or for physical entry or the like, and for establishing user accountability. Identification is the means by which a user provides a claimed identity to a system. A user can be a human user, a computing system, or a process executing on another system. Authentication is the way of proving that you are who you say you are. Authentication within a computing environment encompasses user identity verification, transmission origin authentication, content authentication, and detection of tampering. There are three commonly known mechanisms verify a user's identity. One mechanism relies on something a user knows (e.g. personal identification number, password). A second mechanism relies on something a user has (e.g. magnetic stripe card, smart card, authentication token). Another mechanism involves something a user is (e.g. fingerprints, signature, biometrics technologies). The use of an authentication token with personal identification (number/password) or combinations of any two of the above mechanisms constitutes a two-factor authentication method and is considered a strong authentication.

03 The objective of encryption is to provide a measure of security that can ensure a desired level of confidentiality, privacy, and integrity of data. Encryption is a reversible process using cryptographic algorithms and keys to transform plain text data into encrypted data in order to conceal the meaning of the plain text data from unauthorized access. There are many types of encryption schemes, including the standard DES and RSA scheme that are well known in the art.

04 The non-repudiation security objective is intended to provide assurance that a specific action actually occurred. It may comprise any one or more of the following components: non-repudiation of origin, non-repudiation of submission, and non-repudiation of delivery. Non-repudiation controls prevent an individual from denying receipt, submission and/or delivery of a message, data or other commodity.

05 In general, the security functions of authentication, encryption, and non-repudiation are implemented using a cryptographic algorithm. There are two categories of cryptographic algorithms: symmetric and asymmetric. Symmetric algorithms use the same secret key to encrypt and decrypt a document. Asymmetric algorithms use two different secret keys: where one is used to encrypt a document only the other can be used to decrypt it. Asymmetric algorithms are also known as "Public Key Algorithms", and the RSA algorithm is one example of such asymmetric algorithm.

06 Figure 1 illustrates a schematic configuration for what is known today as the typical "Electronic Commerce" and "Electronic Transaction" systems. The illustrated arrangement 100 is typically engaged by a user 101 who uses a path 150 (manual, electronic or the like) to operate a portable client device 102 that is in communication with a transaction server 104 via links 151, 152 and 153 and a closed network 103, and/or links 151, 156 and 155 via an open network 105. In order to support two-factor authentication and transactions that require digital signature or other security processing, a peripheral device that functions as a secure element may be attached to a client in a master-and-slave configuration. This secure element may be built into a client (e.g., a built-in SIM chip on the mobile phone) or an add-on peripheral device (e.g., a smart card reader attached to a personal computer (PC), notebook or the like). The secure element provides a secured storage medium for the private keys and other personal credentials needed for two-factor authentication and secure transaction processing. The single client may be one of two generic types of devices, including a "fat" client and a portable or "thin" client. The fat client 106 may be a desktop PC or notebook, where there is no practical constraint on the supply of power, the facility for data or command input, the user interface in the nature of a display and the storage capacity needed for the contemplated transactions. The fat client 106 is suitable for processing content-intensive transactions with long text and complex relationships that need browsing, review and processing. The secret keys used in the security functions for the fat client are stored in a smart card 107 and are accessible via a peripheral smart card reader 108 that is attached to or otherwise in communication with the fat client 106.

07 The portable or "thin" client 102 may be a mobile phone, personal digital assistant (PDA) or similar hand-held device, where there is limitation in power supply, data and command input, display and storage capacity needed for the transaction. Due to these limitations, specialized protocols (e.g., Wireless Access Protocol (WAP)) and infrastructures (i.e. WAP gateway 110, providing links 151, 152, and 156) are needed to support a transaction. Moreover, the portable client is only suitable for the processing of simple transactions with short text. The secret keys used in the security functions may be stored in an imbedded Subscriber Information Module (SIM).

08 The computer network that serves to connect the thin client 102 or fat client 106 to the transaction server 104 can be grouped into 2 categories. A first category involves a "closed network" 103, which involves a network configuration that links up the computing facility within an organization. The closed network configuration uses Local Area Network (LAN) or Wide Area Network (WAN) to link up the computers and servers via links 152, 153 and 154. Usually network firewalls are deployed at any network gateway (e.g., WAP gateway 110) to protect the computing facility from external intrusion and attack. The users are known members of the organization, and the computer systems within the closed network 103 are considered trusted resources.

09 The second category involves an "open network" 105, where the term "open network refers to a network configuration that links up the computing facility across organizations. The open network configuration uses Internet, WAN, leased line connection or dial-up line for connection. The users may be known members of the organization or unknown external parties. The computer systems are considered un-trusted resources, as they are prone to hackers' intrusion or attack on the organizational computing facility. The open network provides connections via links 155, 156 and 157.

10 In the illustrated network environment of Fig. 1, the secured transaction may consist of a standard sequence of processing steps. First, the client (whether "fat" client 106 or "thin" client 102) establishes a connection with the transaction server 104 via the closed network 103 or open network 105. Based on this connection, the client 102, 106 issues a request for service from the transaction server 104 and the transaction server processes and sends a transaction to the client 102, 106, which will process the transaction. Then, a user 101 activates a secured transaction processing by keying-in a personal identification number (PIN) in an activity represented by paths 150 and 158 for thin client 102 and fat client 106, respectively. The client 102, 106

processes and approves the transaction on the basis of secret keys stored in the secured element (smart card 107, for example).

11 However, there are some shortcomings with this single client configuration. First, as the client is directly connected to the network, particularly open network 105, there is risk of security attack. For a fat client 106 configuration, an additional secure element, such as smart card 107 and reader 108, may be required but such devices may not be widely available. Second, the fat client 106 is also an unsecured device and subject to intrusion or other security attacks. Third, the fat client solution is unpopular among mobile users who require mobility, portability and high security for their application systems.

12 In a non-electronic environment, the document is the record of the parties' agreement, and the signature is the stamp of a person's identity, and marks his intention to commit himself legally. However, in an electronic environment, there is no paper, pen or ink, and a face-to-face meeting of the parties in person to conduct the signatory process is inconvenient. The solution is to use electronic communications, and electronic signatures on an electronic record. Electronic signatures may be used to establish the identity of the party who electronically signs the electronic document as a proof of his intention to make certain legal commitments. In an online world, trust and confidence are essential pre-requisites to facilitate electronic commerce. Electronic security is of equal importance.

13 Currently, a public key infrastructure (PKI), as further defined subsequently, is the best available solution to address the technical security requirements of data integrity, confidentiality, availability, user identification and authentication and non-repudiation, for electronic commerce transactions. Smart cards or keys stored on magnetic media (i.e. diskettes) issued by Certificate Authorities (CAs) are used as authentication tokens that contain the subject's private keys. Digital signatures provided by PKI can be used to guarantee that the electronic document was digitally signed, and that there has been no tampering or alteration. Increasingly, a legal framework is being established in many countries to deal with the problem of affording legal recognition of electronic and digital signatures. Such framework will include protocols for setting up of a PKI, and will accord legal sanctions for records, files or documents that are retained in an electronic form. It enables public and private institutions to accept electronic applications and perform electronic transactions in an online world. The framework also clarifies the liability of network service providers for third party consent. One example includes

Singapore's Electronic Transactions Act 1998, and similar examples are believed to exist in Canada, USA and other industrially developed countries.

14 The current electronic application systems in the online world are deployed using ID (Identification tag) and PIN (Personal Identification Number)/Password to identify the subject using the system. Added security involves the issuance of authentication tokens so as to fulfil the objective of a two-factor authentication. However, the rate of adoption of PKI for authentication and digital signature in commercially deployed applications of the government, public and private institutions is low. The reasons for the slow adoption can be attributed to a general lack of awareness, a lack of inter-operability and standards among different CA operators and cross-border certification and the cost and complexity of deployment and maintenance (e.g. PKI smart card deployment and maintenance, smart card reader infrastructure). In short, there is a lack of ease of use and convenience, a lack of consensus on cross-border legal issues, and a lack of demand and strategic applications.

15 PKI is a framework of policies, services, and public key encryption system using digital certificates that provide authentication, integrity of data, confidentiality, and non-repudiation security services. Several standards groups have emerged in the arena of PKI, but PKI based on X.509 Working Group (PKIX) defines the most widely adopted specifications to date. The most basic component of a PKI is the certificate. A certificate is issued to subjects and vouches for the identity of the subject. Subjects are usually people, but can be any end entity that needs to identify itself, such as a Web certificate, which can be used to perform cryptographic operations. The following services are currently commercially available through the use of certificates and their associated key pairs:

16 1. Web authentication and channel privacy. Netscape's Secure Sockets Layer (SSL) and IETF Transport Layer Security (TLS) protocols are examples of mechanisms for establishing a secure channel between a client and a server;

17 2. Signed and encrypted messaging. Electronic mail is an ubiquitous technology where there is a need to ensure that the information in the email is kept confidential and is not altered in transit, termed message integrity. Certificates and their associated keys can be used to encrypt and digitally sign electronic mail messages;

18 3. Signed transactions and form signing. A digital signature can be used to legally bind the signer to the content of a contract or a transaction that has been initiated;

4. Network operating system, host and mainframe authentication. Certificate-based authentication can be used as a universal authentication mechanism to many different system platforms;

5. Remote access. Certificate-based authentication offers a more secure alternative to username/password authentication. This also provides a streamlined solution across different system platforms;

6. Virtual Private Networks. Certificates can be used to authenticate end points in a Virtual Private Network (VPN). VPN allows two or more parties to communicate securely over a public network;

7. File encryption. PKI can be applied to issue certificates that attest to the authenticity of their associated keys to encrypt sensitive data; and

8. Software code signing. This enables developers to digitally sign code so that if it changes in any way, the receiver will be made aware of it.

PKI is put in place to issue, distribute and manage the use of digital certificates. Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework defines a certificate policy as a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements."

Several components are required in order for a PKI to complete these tasks. These components are:

Certificate Authorities (CAs). CAs act as trusted third parties in a PKI. CAs issue certificates to subjects. A self-signed certificate identifies the CA itself. The CA is the initial point of trust. CAs are responsible for performing several important tasks including certificate management (issuance, revocation, update and renewal), certificate and CRL publication, and logging of events;

Registration Authorities (RAs). CAs will delegate certain responsibilities to RAs. These include personal authentication, token distribution, token distribution, revocation reporting, name assignment, key generation and archival of key pairs. RAs are used to verify the identity of a subject during the certificate enrolment process;

Certificate Management Protocols (CMPs). These define the specifics of certificate enrolment and the revocation processes. Examples include Public Key Cryptographic Standards (PKCS) and Simple Certificate Enrolment Protocols (SCEP);

29 Certificate Revocations. This is applied when a CA needs to invalidate a certificate prior to its expiration date. Some implementation methods include Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP);

30 Certificate Repositories. This is used to store and distribute certificates and CRLs. Directory Service is an online repository that houses information about objects. X.509 LDAPv2 Schema defines the object classes and attributes that are used in an PKI-enabled directory. Lightweight Directory Access Protocol is used to access information in the directory. Internet X.509 PKI Operation Protocols define data types and naming conventions for transfer of certificates and CRLs using File Transfer Protocol (FTP) or HyperText Transfer Protocol (HTTP); and

31 Time-Stamp Authority (TSA). To reinforce the feature of non-repudiation, TSA is implemented. Internet X.509 Time Stamp Protocol (TSP) describes the use of a time stamping authority.

32 While the foregoing includes a description of a PKI implementation of a single CA, many CA products are capable of issuing large numbers of certificates. Further, large implementations involve multiple CAs. Also, another implementation is Cross-Certification where CAs certify each other in order to establish a lateral trusted relationship, establishing a peer-to-peer model of trust. Cross-Certification offers a feasible implementation for separate PKI implementations to integrate with each other.

33 Figure 2 illustrates a schematic diagram of a system 200 within which current mobile telecommunication devices are used for voice and data communication. These mobile telecommunication services are provided based on Global System for Mobile Communications (GSM), Cellular Digital Packet Data (CDPD) or Code Division Multiple Access (CDMA) specifications. Wireless Access Protocol (WAP) is a protocol that has been optimized for mobile devices. Internet browsing services are provided via WAP. Data Message services are provided using Secure Messaging Service (SMS).

34 The mobile telecommunication broadband services are currently provided via General Packet Radio Service (GPRS); however, the 3G specifications for mobile broadband services are now being specified. The current mobile electronic commerce, conducted between a first user 201 and a second user 207, or content server 204, is facilitated using WAP. The users 201, 207 utilize their respective mobile devices 202, 206 (e.g. WAP-enabled mobile phone, personal digital assistant (PDA)) that can transact in a mobile commerce framework and/or provide

mobile web surfing via a WAP gateway 203 using the wireless network for content transmission. The existing or proposed implementation models based on WAP can be classified into the following three categories:

35 Remote environment. The connection between the Internet content server and the mobile phone device is established via the mobile phone cellular network (e.g. GSM). The Internet access is achieved via the WAP gateway 203. The WAP gateway 203 performs the proxy server functions of protocol conversion from WAP protocols to Internet protocols. Wireless Transport Layer Security (WTLS) is implemented from the mobile phone device 202 to the WAP gateway 203, with Transport Layer Security (TLS) or Secure Sockets Layer (SSL) being used from the WAP gateway 203 via the open network 205 (or closed network - not shown) to the content server 204. Alternately, the content server 204 may host the WAP gateway 203. Here, end-to-end transport layer security is provided from the mobile phone device 202 to the content server 204.

36 Local environment. The connection between the mobile phone device 202 and the local network environment (not shown) is established via WAP-enabled short-range wireless technology (e.g. Bluetooth). WTLS is used to provide server authentication and secure sessions.

37 Personal environment. The connection between the mobile phone device 202 and the Internet browser device is achieved via wireless (e.g. Bluetooth, Infrared) or wired (e.g. Universal Serial Bus (USB)) links. The mobile phone devices 202, 206 are used for authentication and authorization of transactions.

38 A recent mobile telephone initiative is the MeT initiative, as outlined in the "Met Overview White Paper" (version 2.0 dated January 29, 2001) and the accompanying "MeT Core Specification" (version 1.0), and "MeT Retail Shopping" (version A), both issued on February 21, 2001 and available at the MeT website (www.mobiletransaction.org). This is a WAP-based system for local and remote environments, with attendant security measures specified in the standard. Specifically, the mobile device, called a Personal Trusted Device (PTD), has a built-in Security Element, having appropriate keys and certificates. The Security Element is implemented in the form of a combined SIM/WIM card, as a separate WIM smart card, as a removable device carrying WIM functionality or as a hardware Security Element built into the phone or a software-based Security Element in the phone. In the MeT configuration, the PTD is in communication with a front end unit that acts as a "pass through device", located between the PTD and a transaction server, and operating to pass on the message and communications

between the PTD and the server. The pass through device is merely a peripheral and does not play an important role in the transaction process. In fact, the PTD acting as the controller is able to handle the transaction process without the intervention of the pass through device.

39 Other mobile phone-based payment system solutions include the use of SMS messages or Voice Messaging System (VMS) to authenticate and confirm payment transactions. These payment systems are non-WAP-based implementations.

40 A further relevant innovation are the smart cards 107 (Fig. 1), which are used as two-factor authenticators: something that you have (i.e. smart card) and something you know (i.e. personal identification number, password). Smart cards have secure, tamper-resistant memory to store sensitive information such as private keys. Smart cards are able to perform cryptographic computations entirely within the tamper-resistant microprocessor. These features make smart card an ideal complementary component to PKI. For the public/private key generation, the current implementation is either generation of keys within the smart card chip, or the generation of the keys external to the card and loading the keys into the smart card chip. The public key is emitted to the CA. Another feature that makes the smart card ideal for the use with PKI is that it is portable.

41 Nonetheless, there are some shortcomings with smart cards when used with PKI. First, most desktop systems deployed today are not installed with embedded smart card readers. Consequently, this limits the use of smart card to those system that have explicitly installed smart card readers. Second, smart card readers are peripheral devices that need proprietary drivers and/or smart card-aware cryptographic service providers (e.g. PKCS11) must be installed onto the computing system before these can be used. Third, most smart card readers are passive devices and the password to unlock the certificate on the smart card is entered via the input device (e.g. computer keyboard) on the computing device. This input process is open to hacking as the password may be 'hijacked' by keyboard capture virus. This threat has limited the use of PKI for mobile workers. Finally, there are cost issues in deploying a large smart card base for the purpose of a PKI deployment.

42 Nonetheless, smart card reader manufacturers have begun to ship PC/SC-compliant reader drivers that attempt to make the process of adding a reader a plug-and-play operation.

SUMMARY OF THE INVENTION

43 The invention relates to a method, system and apparatus for enabling the features of identification, authentication, encryption and non-repudiation in an electronic commerce transaction between a distributed transaction client device and a transaction server.

44 The invention entails the use of a registered telecommunication-based Portable Intelligent Unit (PIU) as a distributed component with direct communication and transaction with a separate local microprocessor-based Front End Intelligent Unit (FEIU). The Front-End-IU has access to an open or closed network. The Portable-IU and Front-End-IU function as a transaction client that provides one or more purposes of secured transaction that includes identification, authentication, encryption and non-repudiation.

45 A feature of the present invention is an electronic transaction system operative to provide secure communication between a user and a transaction server. The system includes a transaction client having a first unit, accessible by the user and operative to store a security module that activates and provides secured services, and a second unit, in direct communication with the first unit and operative to access and uses said secured services. The combination of applications and services of two units enable the transaction client to provide a secured data transmission. The system also includes a transaction server, in communication with the transaction device and operable to receive the secured data transmission from the transaction client and provide applications and services to the transaction client.

46 Another feature of the present invention is a transaction client for providing secured transactions with a transaction server. The transaction client includes a first unit having a first microprocessor, first data storage and a first communication unit, the first unit having the capacity to store security and processing modules and to execute the modules, and further being operative to communicate with the transaction server. There also is a second unit, comprising a portable registered telecommunication-based device, the second unit having a second microprocessor, second memory and second communication unit, the second unit being operative to provide at least one of authentication, encryption and non-repudiation services. The transaction client further includes a direct connection between the communication units in each of the first unit and second unit.

47 Yet another feature of the present invention is a distributed authentication system for communication between a transaction server and a user. The system includes a portable

information unit, operable by a user and having: a native function module for providing native functions, a native service module for providing native services, a secured memory module for storing at least a secret key, a firewall security module for providing security to the unit against attack, and a security engine module having functions and services for activation of desired security services, comprising at least one of digital signing, verification and authentication. The security engine module is separated and protected by a firewall module and is not accessible by the native function module. There is also a front end unit, operable by the user directly in a normal mode, that uses the secured services from the portable intelligent unit in a secure mode. The front end unit has: a client native function module for providing native functions, a client native service module for providing native services, and a client security engine for processing of services needed for secured data transmissions. Finally, there is a direct communication connection between the portable information unit and the front end unit.

48 A further feature of the present invention is a distributed authentication system providing secure communication between a user and a transaction server. The system has a first intelligent means operative to access stored security keys in order to provide secured message-based authentication, encryption and digital signing; and a second intelligent means in direct connection with the first intelligent means, and in communication with the transaction server. This system is operative to use the secured messages from the first intelligent means and, responsive to a user actuation, to establish at least one of authentication, encryption, verification and digital signing and a secured connection with the networked transaction server, wherein the first intelligent means also is operative to provide secured messages to the second intelligent means. These secured messages are proof of personal credentials for providing authentication, encrypted messages or digital signatures as requested by the user of the first intelligent means for one or more purposes related to a secured transaction, including identification, authentication, encryption and non-repudiation.

49 An additional feature is a method of executing a secure transaction between a transaction client, having a distributed device and a front end device in communication with the distributed device, and a transaction server. The method includes several steps, including a step of initiating a transaction by communicating a request for services by the front end device in the transaction client to the transaction server, processing a transaction at the transaction server and sending the transaction to the front end device. There also is a step of verifying the transaction at the front end device. A further step is authorizing a transaction using a secure service and providing a secured message at the front end unit, and approving a transaction.

50 The invention also includes a transaction system for providing secure communication between a user and a transaction server. That system includes a first intelligent means operative to access stored security keys and responsive to a user actuation to establish at least one of authentication, encryption, identification and digital signing. It also includes a second intelligent means in direct connection with the first intelligent means via a non-WAP-based link, and in communication with the transaction server. The second intelligent means uses secured messages from the first intelligent means to establish a secured connection with the networked transaction server.

51 Finally, the invention includes a portable hand set having a telecommunications unit for direct communication with an intelligent front end unit, an input/output unit operative by a user for inputting transaction information, a processor and memory storing personal secret key information, a secrecy engine for accessing the secret key information in response to a user input information and for providing secured messages to be processed by second intelligent means or other device in a two-factor authentication and secure transaction processing.

BRIEF DESCRIPTION OF THE DRAWINGS

52 Figure 1 is an illustration of a schematic configuration of an electronic commerce framework.

53 Figure 2 is an illustration of a schematic configuration of a mobile telephone services framework.

54 Figure 3 is an illustration of a schematic configuration of a secure communication framework in accordance with the present invention.

55 Figure 4 is an illustration of a schematic diagram of components and relations among those components in accordance with the present invention.

56 Figure 5 is an illustration of the flow of activity among a user, PIU, FEIU, closed/open network and transaction server in a normal mode and a secure mode, in accordance with the present invention.

57 Figure 6 is an illustration of a local system implementation of the present invention.

DETAILED DESCRIPTION OF THE EMBODIMENTS

58 Figure 3 is a schematic illustration of a system and its operational method that implements the invention. A user 301 accesses the system 300 in order to communicate with a transaction server 304 so that an electronic transaction or other secure transaction may be conducted via a closed network 303 (path 355, 357) or open network 305 (path 354, 356). The user 301 can access a front-end intelligent unit (FEIU) 302 directly (path 351), or access both FEIU 302 and portable intelligent unit (PIU) 310 together (path 352, 353 and path 351), so that a secure communication can be conducted with the transaction server 304. The PIU 310 is connected to the FEIU 302 locally via a direct connection 353 and, in an exemplary embodiment, comprises a portable unit 311 that is protected by a built-in firewall 312. In an exemplary secure network implementation, PIU 310 can only communicate with the FEIU 302, and is operative to provide secured messages to the FEIU 302 for one or more purposes that relate to the implementation of secured transactions, including identification, authentication, encryption and non-repudiation. In the exemplary secure network implementation, the PIU 310 does not access the closed network 303 or open network 305 directly.

59 The electronic transaction that may be conducted over the disclosed system can be classified as "normal transaction" or "secured transaction" and the data transmitted between the user 301 and the transaction server 304 can be classified as "incoming transmission" and "outgoing transmission". The incoming transmissions are the transactions transmitted from transactions server 304 to user 301 whereas the outgoing transmissions are the transactions transmitted from user 301 to transaction server 304. All incoming transmissions, both normal and secured transactions, and the outgoing normal transactions are handled by the FEIU 302 by a user's direct access along path 351. The PIU 310 is not used for the incoming normal and secured transactions and outgoing normal electronic transaction. Of course, as would be understood by one skilled in the art, the PIU 310 may be a customized device or a conventional generic communication device with specialized programming, such as a mobile phone, that may be used for a variety of communication purposes unrelated to the conduct of electronic transactions. The specialized programming in the PIU 310 will enable the conduct of the processes for the conduct of secured electronic transactions, as subsequently disclosed in connection with Fig. 5.

60 In accordance with an exemplary embodiment of the present invention, user 301 uses both the FEIU 302 and the PIU 310 to conduct secured electronic transactions via paths 352, 353

and 351. The combination of a FEIU 302 and PIU 310, as separate but cooperating elements that form a "distributed transactional client" 306, results in a distributed configuration that forms a secured client for use in the conduct of secured transactions, particularly those conducted over a network. The distributed configuration securely isolates the PIU 310, which is responsible for providing the secured message functions for authentication, encryption and non-repudiation. The distributed configuration and the portability of PIU 310 minimize the possibility of intrusion attack via the network connection. The built-in firewall 312 further reduces the risk of Trojan horse and other security attacks.

61 Figure 4 is a schematic diagram representing the generic configuration 400 of the components of the transactional client 306 that forms a key unit of the present invention, and their operating relationships. The PIU 410 in Figure 4 is a telecommunication device (i.e., mobile phone, PDA or specialized device) that is registered for use with a licensed telecommunication service operator. The PIU 410 has the capability to store and execute security and processing modules. It communicates with the FEIU 420 by a non-WAP-based communication link via direct connection 451 using wireless technologies (e.g. infrared, Bluetooth) or wired means (e.g. Universal Serial Bus (USB), Serial Port, Parallel Port). The PIU 410 provides secured messages for mutual authentication, secured data transmission and digital signing, and comprises several components.

62 One (as shown) or more Portable Information Unit-enabled Subscriber Information Modules (PIU-enabled SIM) 411 provide the secured memory storage that includes password protected access to store the secret keys and other personal credentials needed for two-factor authentication and secure transaction processing. The mobile telephone subscriber's information may be stored in the PIU-enabled SIM(s) 411 or, as would be understood by one skilled in the art, may be stored in whole or in part in a separate secured memory storage (not shown). The content of the PIU-enabled SIM 411 may be encoded on a smart card, soft-coded/hard-coded on board circuitry of the PIU 410 or equivalent device, or may be stored in an external secured storage medium.

63 A Firewall Security Module (FSM) 412 is the security module that has security features to protect the PIU 410 from security attacks. It serves to filter data communication that occurs between the PIU 410 and the Front-End-IU (FEIU) 420. The FSM 412 will alert the user when any attempted or actual breach of a secured transmission is encountered.

64 The Native Functions Module (NFM) 413 provides native functions for the PIU 410. These functions include, but are not limited to, input and output functions for the keypad, digital signing button 416, touch screen (if any), audio alert or message, and display screen.

65 The Native Service Module (NSM) 414 provides the native services that come with or are provided by the PIU 410. These services include the conventional mobile phone functionality, like voice and data communications.

66 A Security Engine Module (SEM) 415 is connected to the PIU-SIM 411 and contains functions and services needed for activation of secured services, such as authentication, verification and digital signing. The SEM 415 is separated from the NSM 414 and the outside world by the FSM 412, and is not accessible by NSM 414. Thus, the NSM 414 cannot be used as an entry point to compromise the secure services of the SEM 415.

67 Another feature on the SEM 415 in PIU 410 is a periodic transmission of "token evidence". After successful completion of authentication, the SEM 415 will continuously transmit a secured signal at a regular interval to FEIU 420 as an evidence that the PIU 410 is connected to the FEIU 420. This feature can be used in virtual private network application (VPN) or other remote computing application where the transaction server that require to periodically perform security verification on the transactional client. The signal is generated within the SEM module 415, and does not involve the PIU-enabled SIM 411, and it uses the security feature in of FSM 412 for the secure messaging. It also uses the duplex transmission feature in PIU 410 that will be described subsequently.

68 The PIU 410 features a duplex processing mode that allows the user to transmit a token evidence signal to FEIU 420 and to use other capabilities of NSM 414, such as voice communication, at same time. It allows PIU 410 to switch between secure and normal mode periodically, e.g., by example and without limitation, once every 1 minute, to support both NSM 414 services and token evidence transmissions.

69 The PIU 410 features a digital signing button 416 that is provided for the user to activate the authentication and/or digital signing features. A separate button is provided for this purpose in the exemplary embodiment, but as would be apparent to one skilled in the art, based on appropriate programming, that combinations of conventional keypad keys or touch screen icons may be used to provide the activation function.

70 The Front-End-IU (FEIU) 420 is a local microprocessor-based device (e.g. personal computer, notebook, PDA, Internet browsing device, or the like) that has access to an open or

closed network. The FEIU 420 has the capability to store and execute security and processing modules. It communicates with the PIU 410 via secure direct connection 451 using wireless technologies (e.g., infra-red, Bluetooth) or wired means (e.g., Universal Serial Bus, Serial Port, Parallel Port), under the protection of the firewall FSM 412. It uses the secured services from PIU 410 for mutual authentication, secured data transmission and digital signing.

71 The Front-End-IU 420 comprises several components, including a Client Native Functions Module (CNFM) 421. CNFM 421 provides the native functions of the FEIU 420, such as the input and output functions of the FEIU 420. Another component is the Client Native Service Module (CNSM) 422. CNSM 422 provides the native services for the FEIU 420, including all the executable programs and functions stored in FEIU 420. There also is a Client Security Engine Module (CSEM) 423, which is a PIU-enabled unit that contains the client security software for the processing of services needed for secured data transmission, and the processing of services between the PIU 410 and the FEIU 420. The processing includes the preparation of transactions for digital signature and encryption using a message digest program, such as MD5 algorithms, and symmetric key encryption.

72 The FEIU 420 manages and processes the secured transactions needed for the provision of security services. It communicates with the open network 450 or closed network (not shown), and enables the establishment of a secured data transmission with the network via link 452, with a further connection to the transaction server 440 via link 453. The FEIU 420 also establishes a secure connection with the PIU 410.

73 The PIU module 410 interfaces and communication, the FEIU module 420 interfaces and communication, the communication between the PIU 410 and FEIU 420, and the communication between the FEIU 420 and the open network 450 or the closed network (not shown) are all governed by a set of secured protocols called the Secured Communication Protocol (SCP). This protocol set governs services that enable password access control, mutual authentication, secured data transmission, intrusion handling (e.g., hacking, playback attack, etc.) and error handling, as would be understood by one skilled in the art.

74 Using a modular design, the PIU 410 and FEIU 420 can store multiple sets of security engine and secret keys in the respective PIU enabled SIM 411, SEM 415 and CSEM 423. The security engines can use both symmetric and asymmetric cryptographic algorithms by encapsulating the cryptographic algorithm in the SEM 415. These multiple sets of security engine and secret keys allows one distributed transactional client 410 (PIU 410 and FEIU 420)

to provide secure transactions in multiple application domains. A unique application identification (app-ID) is assigned to each set of security engine and secret keys in the PIU enabled SIM 411, SEM 415 and CSEM 423 . The app-ID is also used by the FSM 412 in PIU 410 to process and filter data transmissions between the CSEM 423 in FEIU 420 and the SEM 415 in PIU 410. The collaboration processing among the CSEM 423, FSM 412, SEM 415 and PIU enabled SIM 411 form a distributed configuration establishing a distributed transaction client 460. The management and distribution of app-ID is governed by the SCP.

75 Each secure application deployed using the distributed transactional client 460 has three essential components, a secret key component, a security engine component and a server component.

76 The secret key component involves the management and distribution of a secret key. With reference to Figs. 3 and 4, a unique secret key is distributed to user 301 and transaction server 304. The secret key for user 301 is stored in the PIU-enabled SIM 411 in PIU 410 and the secret key for the server 304 is stored in the server backend system using smart card or other secured storage, as would be known to one skilled in the art.

77 The security engine component consists of application modules for secure applications according to SCP specifications, and are deployed on the SEM 415 in PIU 410 and CSEM 423 in FEIU 420.

78 The server component is the system deployed, including the secret key component, at the service provider's premises that provides applications and services over open/ closed network.

79 Notably, the method and system of the present invention is implemented in a manner that is distinctly different from the mobile commerce implementation of authentication and payment services that are deployed or proposed to be deployed using WAP or WAP-related protocols, standards and specifications, as exemplified by the system of Figs. 1 and 2. The present method is a non-WAP-based implementation that is designed to fulfill the functions of identification, authentication, encryption and digital signatures in an electronic commerce framework where electronic transactions must be securely conducted.

80 As earlier noted, the processes that effect electronic transaction implementations can be divided into 2 main categories, "normal transactions" and "secured transactions". In an exemplary process illustration, the necessary system hardware configuration and network of Figs. 3 and 4 is setup, and the appropriate client application that processes the normal transaction is implemented onto the CNSM 422 and CNFM 432 in FEIU 420. The normal

transactions, as illustrated in Fig. 5, involve the FEIU 420 and the transaction server 440 that is connected to the open network 450 or the closed network (not shown). The normal transaction is handled by the CNFM 421 and CNSM 422, and does not require the use of the PIU 410. With reference to Figs. 3 and 5, in step 501, a user 301 can directly input an outgoing normal transaction to the FEIU 302 over link 351, and effect communication in steps 502 and 503 to send the outgoing normal transaction to the transaction server 304 via the closed network 303 or the open network 305. Similarly, in steps 504 and 505, the transaction server can send incoming normal transactions via the closed network 303 or the open network 305 to the FEIU 302. In step 506, the user 301 can receive the incoming normal transaction over link 351.

81 The distributed transactional client 306 together with the PKI infrastructure can provide secured transactions that require identification, authentication, encryption or digital signing. The distributed transactional client 306, combines use of the FEIU 302 and the PIU 310 via a direct connection on link 353, to provide the described services of authentication, secured data transmission and digital signing. This service enables a secure communication with the transaction server 304 via the open network 305 or the closed network 303. The secret keys used in the secured transactions are stored in a digital certificate issued to both the user 301 and the transaction server 304. Specifically, with reference to Fig. 4,. the digital certificate for user 301 is securely stored in the password protected PIU-enabled SIM 411. A certificate client with app-ID tag that accesses and uses this digital certificate to provide identification, authentication, encryption and digital signing is implemented in SEM 415 in PIU 410. CSEM 423 in Front-end IU 420 includes a front end secure client with the same app-ID tag, and supports transaction input, transaction packaging and communication with the SEM 415 in PIU 410. The communication between SEM 415 in PIU 410 and CSEM 423 is made secure by FSM 412 in PIU 410 using the app-ID in SEM 415 .

82 Because of its isolation and the password protection, the SEM 415 can effect a secure access to the one or more PIU-enabled SIMs 411 to extract stored subscriber information, secret keys and other personal credentials. This secure access offers strong two-factor authentication and secure transaction processing, including digital signing. The achievement of a secured transaction, using the PIU 410 to connect to the FEIU 420 for communication with the transaction server 440, regardless of the chosen network connection, is based on a protocol that may be divided into 4 phases: a transaction initiation phase, a visual verification phase, an authorization phase and a transaction approval phase. The execution of these four phases on the

basis of activity among the user 301, PIU 410, FEIU 420, open/closed networks and transaction server 440 is illustrated in Fig. 5.

83 The transaction initiation phase 510 (Phase 1) is based on a communication between the FEIU 420 and the transaction server 440 via the open and/or closed network. In this phase, the FEIU 420 is operating in the networked mode 551 and the PIU 410 is not operatively connected to the FEIU 420. This phase comprises several steps or processes. First, in steps 511 and 512, respectively, the CNSM 422 in the FEIU 420 establishes a connection with the transaction server 440 via the open/closed network. Then, with the delay 513 inherent in determining that the connection has been made, during steps 514 and 515, the CNSM 422 in the FEIU 420 issues a request for transaction service from the transaction server 404. The desired transaction service may be selected by a user on the basis of an input to the FEIU 420 keyboard (not shown) that is connected via the CNFM 421 and the transaction client component in CNSM 422. During period 516, the transaction server 440 processes and sends, according to steps 517 and 518, the specifically requested transaction to the FEIU 420. The requested transaction includes proof of identity of the transaction server 440 using the server's digital certificate. The CNSM 422 in FEIU 420 will receive and then process the transaction. In step 519, the CNSM 422 retrieves the public key from a CA server via the open network (not shown) to verify the identity of transaction server 440. Upon verification, CNSM 422 will process the incoming transaction in step 519A and present the transaction for user visual verification, thereupon concluding the Phase 1 transaction initiation.

84 In the second phase 520 (Phase 2), there is a visual verification that occurs between the user and FEIU 420. In step 521, the user makes a visual verification with respect to the validity of the secured transaction on a display of the FEIU (See Fig. 3, display portion on FEIU 302). The verification may be made on the basis of text or symbols that uniquely identify the transaction that has been provided, and the user's notation of which transaction originally had been requested.

85 The third phase 530 (Phase 3) is the transaction authorization phase, which occurs between the FEIU 420 and the PIU 410. At this stage, the FEIU 420 has the downloaded transaction and is only operating locally 552, as the communication with the transaction server 440 is temporarily suspended. The PIU 410 alone may initiate the secure service feature of the transaction. FEIU-initiated connection to the PIU 410 is not allowed for security reasons. The "secured service request" that is established will involve data transmitted from the FEIU 420 to the PIU 410 for service requests for authentication, encryption and digital signing. The "secured

message" refers to data and services processed and transmitted by the PIU 410 to the FEIU 420 for the services of authentication, encryption and digital signing.

86 This third phase comprises several steps in sequence. First, in step 531, the PIU 410 establishes or activates a physical connection 451 with the FEIU 420, that connection being wired or wireless. A delay 522 may be required to confirm the operational existence of the link. Then, in step 532, the user activates the PIU 410 by pressing a digital sign button 416 on the device. In response, in step 533, the SEM 415 in the PIU 410 establishes a secured connection with the CSEM 423 in FEIU 420. Then in step 534, the CSEM 423 in the FEIU 420 sends a secured service request to the SEM 415 in the PIU 410. The transmitted service request represents the security requirement established by the transaction received at the FIEU 420 from the transaction server 440. These transmissions are checked and filtered by the FSM 412 in step 535 and, if safe and acceptable, the SEM 415 in the PIU 410 activates a secured service by service request type.

87 Next, in step 536, the user verifies the secured service request on the PIU 410 and, if proper, the user approves the transaction by keying in a personal identification number (PIN) using a keypad on the PIU 410 in step 537. The PIN will unlock the user digital certificate stored in the PIU-enabled SIM 411. On the basis of the digital certificate, the SEM 415 in the PIU 410 processes the secured service and sends the required secure message to the CSEM 423 in the FEIU 420 in step 538. Finally, the PIU 410 terminates the connection with the FEIU 420 in step 539.

88 The final or transaction approval phase 540 is conducted between the FEIU 420 and the transaction server 440. At this stage, the FEIU 420 is operating in a "network" mode 553 and the communication with PIU 410 is dropped. The FEIU 420 has received a secure message from the PIU 410 and generates a secured transaction reply. The term "secured transaction reply" refers to the data transmission between the FEIU 420 and the transaction server 440 in the open/closed network for conducting a transaction with an authentication reply, encrypted message and/or digital signing. The transaction approval phase also comprises several processes.

89 First, in step 541, the CSEM 423 in the FEIU 420 packages the secured message received from the PIU 410 into a transaction reply. That transaction reply may be an encrypted message, or authentication based on the proper entry of a PIN and release of stored secret key, or digital signature, in a format that is recognized by the transaction server, preferably using the SCP protocol as previously noted. Then, in steps 542 and 543, the FEIU 420 sends the secured

transaction to the transaction server 440. This completes the last of the four phases and the secure transmission process ends in step 544.

INDUSTRIAL APPLICABILITY

90 The system and method of the presently disclosed invention, or its derivatives, are capable of industrial application and commercial deployment.

91 The disclosed system and method or its derivatives can be used to deploy industrial applications or commercial developments having any one of three system configurations: Remote Closed Network configuration; Remote Open Network configuration; and Direct Closed Network configuration. The remote closed and remote open networks would be apparent from Figs. 3 and 4, while the direct closed network is seen in Fig. 6. There, a user 601 can access a FEIU 602 for direct normal communication with a transaction server 604, or via a PIU 610, having a hand held unit 611 served by a firewall 612, for secure access. Such system could be used for authorized entry to facilities.

92 Both symmetric and asymmetric cryptographic algorithms can be used to deploy applications in remote closed network configurations. An example of the symmetric cryptographic algorithms deployed over the remote open network configuration is remote computer application access. In this regard, the user can use the symmetric keys stored in the PIU 410 for access authentication and gain access to computing applications residing in the remote server. An example of the asymmetric cryptographic algorithms deployed over the remote closed network configuration is a remote transaction approval system. The user can access the remote transaction server 440 over the local area network and use the PKI based digital signature keys to sign and approve a transaction.

93 Using the encryption functions in the invention, a secure communication channel can be established between the FEIU 420 and the remote transaction server 440 over the open network 450. All applications deployed on the remote closed network configuration can be deployed over the remote open network configuration that has access through a secure communication channel. Both symmetric and asymmetric cryptographic algorithms can be used to deploy applications using the direct closed network configuration.

The disclosed system and method or its derivatives can be use to deploy a security system using PKI digital certification to support authentication, encryption and digital signature.

94 The disclosed system and method or its derivatives can be used to deploy a security system using symmetric encryption that supports an electronic purse and a two-factor access token.

95 The disclosed system and method or its derivatives can be used to deploy for direct payment at the Point-Of-Sales system (POS system) at a merchant establishment. The Front-End-IU functions as the POS system and the user uses the Portable-IU to approve transactions using a PKI-based digital signature. The POS system sends the signed transaction to the transaction server for verification and approval.

96 The disclosed system and method or its derivatives can be used to deploy Virtual Private Network application (VPN) and Single Sign login, the FEIU functioning as a remote client accessing the transaction server over an open network. The token evidence feature provides additional security. The communication between FEIU and transaction server will automatically cut off when the PIU is removed.

97 While the present invention has been disclosed in connection with one or more preferred method or system embodiments, it is not limited thereto but is instead delimited by the claims, and the applicant intends to acquire a full scope of protection based upon those claims under applicable principles of law.

CLAIMS

1. An electronic transaction system operative to provide secure communication between a user and a transaction server, comprising:

a transaction client having a first unit, accessible by said user and operative to store a security module that activates and provides secured services, and a second unit, in direct communication with said first unit and operative to access and process said secured services, said transaction client providing a secured data transmission; and

a transaction server, in communication with said transaction client and operable to receive said secure data transmission from said transaction client and provide applications and services to said transaction client.

2. The secure electronic transaction system of claim 1, wherein secure data transmission is based upon a secured protocol.

3. The secure electronic transaction system of claim 2, wherein said secured protocol is the standard SCP protocol.

4. The secure electronic transaction system of claim 1, wherein said first unit comprises a portable unit and said second unit comprises an intelligent front end unit (FEIU), said FEIU and portable unit being coupled by a communication link.

5. The secure electronic transaction system of claim 4 wherein said secure service comprises the provision of a secure message, and said FEIU is operable to communicate with said transaction server in a secure mode on the basis of the secured message from said first unit.

6. The secure electronic transaction system of claim 1 further including at least one of an open network and a closed network, said at least one network being operative to provide a communication link between said second unit and said transaction server.

7. The secure electronic transaction system of claim 1, wherein said transaction client is further operative to provide at least one of mutual authentication, token evidence, encryption and digital signing.

8. The secure electronic transaction system of claim 1 wherein said second unit is directly accessible by a user to conduct a non-secure communication with said transaction server.

9. The secure electronic transaction system of claim 1 wherein said transaction client is operative to implement a secure transaction without use of a specialized Wireless Access Protocol or Wireless Access Protocol infrastructure, particularly a WAP gateway.

10. A transaction client for providing secure transactions with a transaction server comprising:

a first unit having a first microprocessor, first data storage and a first communication unit, said first unit having the capacity to store security and processing modules and to execute said modules, and further being operative to communicate with said transaction server;

a second unit, comprising a portable registered telecommunication-based device, said second unit having a second microprocessor, second memory and second communication unit, said second unit being operative to provide at least one of authentication, token evidence, encryption and non-repudiation services; and

a direct connection between the communication units in each of said first unit and said second unit.

11. The transaction client of claim 10, wherein said second unit further includes a firewall.

12. The transaction client of claim 10 wherein said direct connection comprises a wired or wireless communication link.

13. The transaction client of claim 10 wherein said second unit comprises a selector, operative by a user in conjunction with a native function module, to activate authentication and digital signing functions.

14. The transaction client of claim 10 wherein said first communication unit includes a first circuitry for communication with the second communication unit in said second unit and a second circuitry for communication with at least one of an open and a closed network.

15. A distributed authentication system for communication between a transaction server and a user, comprising:

a portable information unit, operable by a user and having:

a native function module for providing native functions;

a native service module for providing native services;

a memory module for storing at least a secret key;

a firewall security module for providing security to said unit against attack; and

a security engine module having functions and services for activation of desired security services, comprising at least one of digital signing, verification and authentication;

wherein, said security engine module is separated and protected by a firewall module and is not accessible by said native function module;

a front end unit, having:

a client native function module for providing native functions;

a client native service module for providing native services; and

a client security engine for processing of services needed for secured data transmission; and

a direct communication connection between said portable information unit and said front end unit.

16. A distributed authentication system as set forth in claim 15, wherein said front end unit comprises a display unit, said display unit providing a display of a secured transaction for visual verification by a user.

17. A distributed authentication system as set forth in claim 15, wherein said security engine of said portable information unit and said security engine of said front end unit are in communication via said firewall security unit.

18. A distributed authentication system as set forth in claim 15, wherein said portable information unit duplex processing mode that switch between secure and normal mode periodically to support voice communication and toke evidence processing.

19. A distributed authentication system as set forth in claim 15 support multiple secure applications with symmetric and asymmetric secret keys.

20 A distributed authentication system as set forth in claim 17, wherein said portable information unit comprises at least one of a symmetric and an asymmetric cryptographic algorithm, said algorithm being stored in said memory module.

21. A distributed authentication system as set forth in claim 15, wherein said native function module is operative to serve the actuation of a digital signing button, said button being operable by a user to activate the establishment of a connection with the front end unit, and a keypad, said keypad being operable by a user to input a personal identification number.

22. A distributed authentication system as set forth in claim 15, wherein said secret keys are at least one of a PKI digital certificate, User ID, password or other form of personal credential.

23. A distributed authentication system as set forth in claim 15, wherein said secret key is accessible by said security engine module of said portable information unit and is used to perform a security function of at least one of authentication, encryption and digital signature.

24. A distributed authentication system as set forth in claim 23, wherein said security function is used as a basis for securely transmitting data from said portable information unit to said security engine module of said front end unit.

25. A distributed authentication system as set forth in claim 24, comprising a plurality of modules operative to store multiple sets of security engines and secret keys.

26. A distributed authentication system providing secure communication between a user and a transaction server, comprising:

first intelligent means operative to access stored security keys and responsive to a user actuation to establish at least one of authentication, encryption and digital signing; and

second intelligent means in direct connection with said first intelligent means, and in communication with said transaction server, for providing a secured service to said first intelligent means and a secure connection with the networked transaction server,

wherein said first intelligent means also is operative to provide secure messages to said second intelligent means using said stored security keys.

27. A method of executing a secure transaction between a secure client, having a distributed device and a front end device in communication with said distributed device, and a transaction server comprising:

initiating a transaction by communicating a request for services by said front end device in said secure client to said transaction server, processing said transaction at said transaction server and sending said transaction to said front end device;

verifying said transaction at said front end device;

authorizing said transaction using a secure service and providing a secure message at said front end unit, and

approving said transaction.

28. The method of claim 27, further comprising selecting between a normal mode, wherein communications are conducted by a user directly with said front end device, and a secured mode, wherein communications are conducted by a user both directly with said front end device and via said portable unit.

29. The method of claim 27 further comprising operating said front end device in a local mode, without connection to said transaction server, during said authorizing step.

30. The method of claim 27 further comprising operating said front end device in a network mode, with connection to said transaction server, during said approving step.

31. The method of claim 30, wherein said authorizing step further comprises suspending communication between said front end unit and said transaction server.

32. The method of claim 27 wherein said authorizing step further comprises:

establishing a secure connection between said distributed device and said front end device;

sending a secure service from said front end device to said distributed device;

approving a transaction, including using a first code to obtain a second code stored in said distributed device, processing a secured service with said second code and sending a secured message to said front end device.

33. The method of claim 32 wherein said first code comprises a personal identification number and said approving step further comprises (1) a user entering said number and (2) a security engine in said distributed device using said number to remove said second code from a storage in said distributed device.

34. The method of claim 33 wherein said second code is used to process a secured service sent from said front end device to said distributed device.

35. The method of claim 27 wherein said approving step comprises: operating said front end device in a networked mode without communication with said distributed device, and providing a secured transmission reply to said transaction server.

36. The method of claim 35 wherein said secured transmission reply is sent via at least one of an open network and a closed network.

36. A non-WAP-based mobile communication transaction system for providing secure communication between a user and a transaction server, comprising:
first intelligent means operative to access stored security keys and responsive to a user actuation to establish at least one of authentication, encryption, identification and digital signing; and
second intelligent means in communication with said first intelligent means via a first non-WAP-based link, and in communication with said transaction server via a second non-WAP-based link, for providing a secured service to said first intelligent means and a secure connection with the networked transaction server.

37. The non-WAP-based mobile communication transaction system of claim 36, wherein said communication between said first intelligent means and said second intelligent means is provided by a direct connection.

38. The non-WAP-based mobile communication transaction system of claim 37, wherein said direct connection is at least one of a wireless and a wired connection.

39. The non-WAP-based mobile communication transaction system of claim 38, wherein said wireless connection is one of infra-red and Bluetooth.

40. The non-WAP-based mobile communication transaction system of claim 38, wherein said wired connection comprises at least one of a universal serial bus, serial port and parallel port.

41. A portable hand set comprising:

a telecommunications unit for direct communication with an intelligent front end unit,

an input/output unit operative by a user for inputting transaction information, a processor and memory storing personal secret key information,

a secrecy engine for accessing said secret key information in response to said user input information and for providing two-factor authentication and secure transaction processing for said intelligent front end unit.

42. The portable handset of claim 41, wherein said portable hand set is at least one of a mobile telephone and personal digital assistant.

43. The portable handset of claim 41, further comprising in said input/output unit a digital signing switch, said switch being a unique button to initiate authentication and signing, and a keypad for inputting a personal identification number.

44. The portable handset of claim 41, wherein said telecommunications unit is operative to communicate at least without use of a wireless access protocol.

Fig. 1

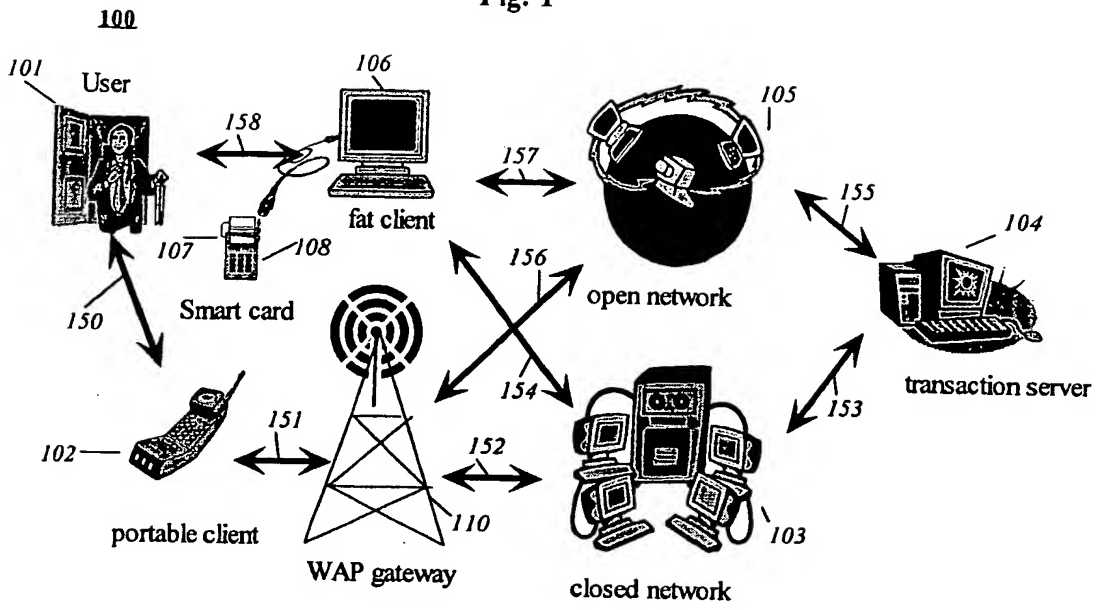

100
101
User
106
158
fat client
105
157
155
104
107
108
Smart card
156
open network
150
transaction server
154
153
102
151
152
portable client
110
WAP gateway
103
closed network

Fig 2

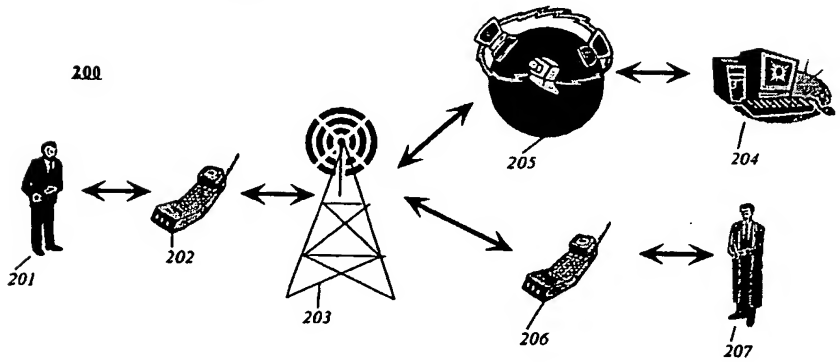

200
205
204
201
202
203
206
207

Fig. 3

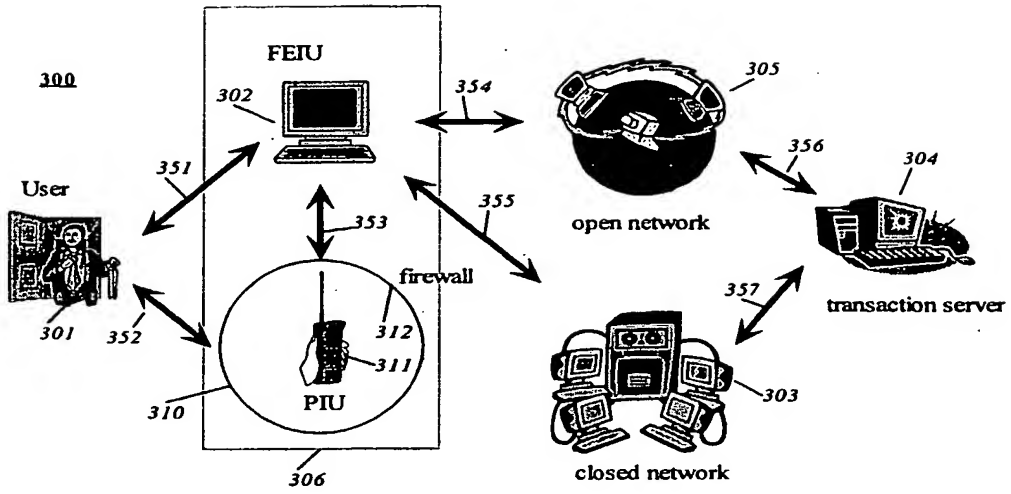

300
FEIU
302
354
305
356
304
351
User
353
355
open network
transaction server
firewall
357
312
311
301
352
PIU
303
310
306
closed network

Fig. 4

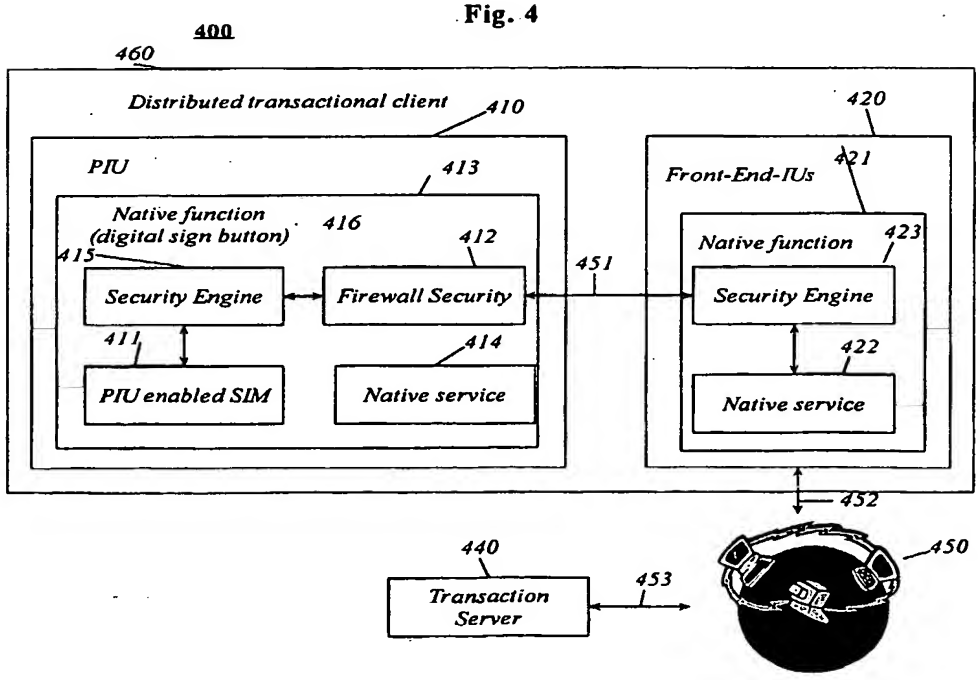

400
460
Distributed transactional client
410
420
PIU
413
421
Front-End-IUs
Native function
(digital sign button)
416
412
423
415
Native function
451
Security Engine
Firewall Security
Security Engine
411
414
422
PIU enabled SIM
Native service
Native service
452
440
450
453
Transaction
Server

Fig 5

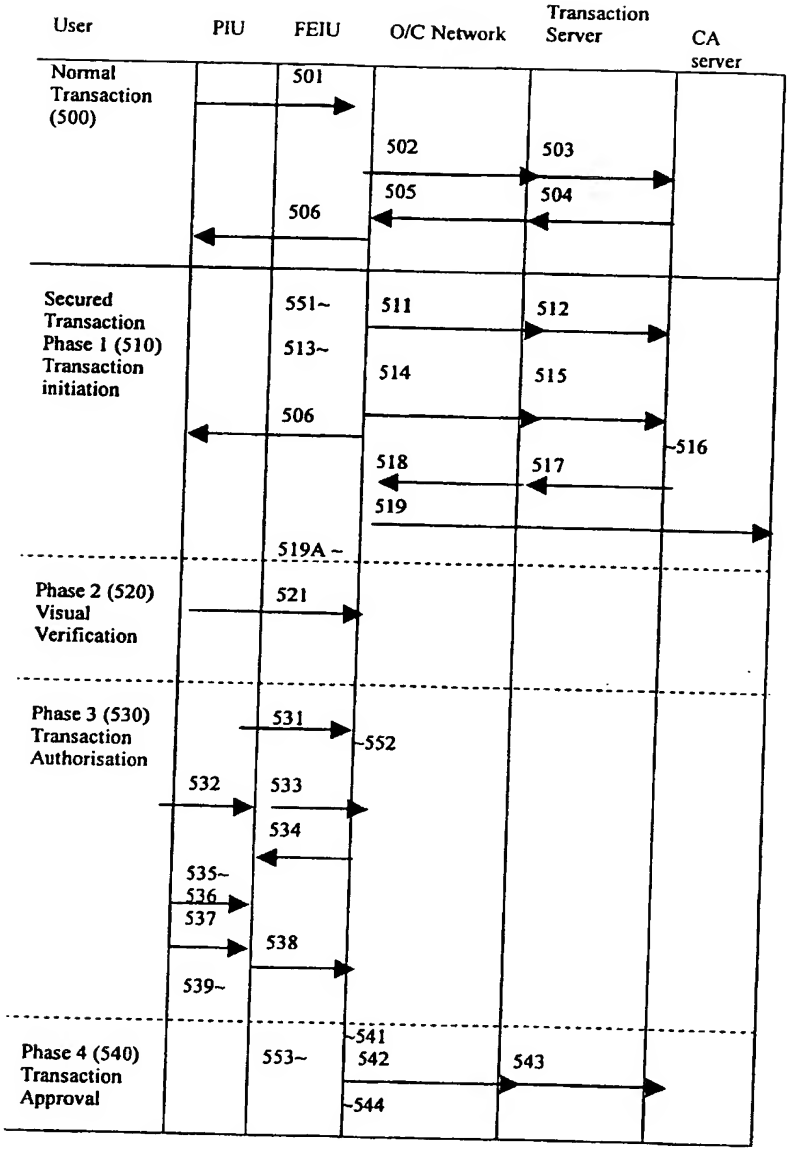
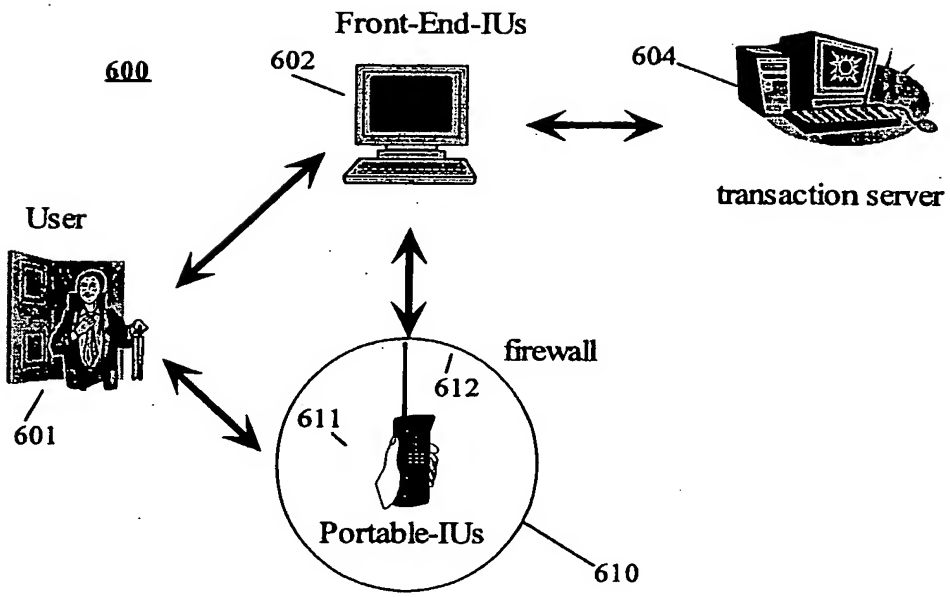

User
PIU
FEIU
O/C Network
Transaction Server
CA server
Normal Transaction (500)
501
502
503
505
504
506
Secured Transaction Phase 1 (510) Transaction initiation
551~
511
512
513~
514
515
506
516
518
517
519
519A ~
Phase 2 (520) Visual Verification
521
Phase 3 (530) Transaction Authorisation
531
552
532
533
534
535~
536
537
538
539~
541
Phase 4 (540) Transaction Approval
553~
542
543
544

Fig. 6


Front-End-IUs
600
602
604
transaction server
User
firewall
612
611
601
Portable-IUs
610

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SG 02/00049

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 78070 A (ERICSSON TELEFON AB L M) 21 December 2000 (2000-12-21) abstract page 2, line 28 -page 4, line 24 page 7, line 1 -page 8, line 2 --- -/--	1,2, 6-10, 12-14, 27-30, 32-38, 41-44

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 January 2003	30/01/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Adkhis, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SG 02/00049

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	BORCHERDING M: "MOBILE SECURITY - AN OVERVIEW OF GSM, SAT AND WAP" LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER VERLAG, NEW YORK, NY, US, vol. 1740, 30 November 1999 (1999-11-30), pages 133-139, XP002951479 ISSN: 0302-9743 abstract page 135, line 27 -page 139, line 35	1,2, 6-10, 12-14, 27-30, 32-38, 41-44

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int...ional Application No
PCT/SG 02/00049

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0078070 A	21-12-2000	NO 992839 A	11-12-2000
		AU 6031200 A	02-01-2001
		EP 1186183 A1	13-03-2002
		WO 0078070 A1	21-12-2000